PRICEWATERHOUSECOOPERS

HIPAA Security and Privacy Rules: Working Together

By: Tom Hanks
Director Client Services
Health Care Practice

Tom.Hanks@us.pwcglobal.com
Phone: (312) 298-4228

October 23, 2001

PRICEWATERHOUSECOOPERS

HIPAA Security and Privacy Rules: Working Together

Thomas L. Hanks

October 23, 2001

Overview

The health care industry typically treats the Privacy and Security rules, promulgated under the Health Insurance Portability and Security Act of 1996 (HIPAA), as two unrelated regulations that are independent of each other. The final Privacy rule was published April 14, 2001, and the industry is still pondering over the proposed Security rule that was published as a Notice for Proposed Rule Making (NPRM) in 1998, while waiting for final Security rule to appear in late 2001. However, We do not have to wait for the Security rule to gain an understanding of the security requirements.

The Privacy rule mandates covered entities provide for the security of protected health information. CFR 45 § 164.530(c) states that, "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information". Since the final Security rule will not conflict with the provisions in the Privacy rule, we can reliably look to those areas in the Privacy rule related to the safeguarding of protected health information (PHI) for guidance on what to expect from the final Security rule. In fact, if we never had a Security rule, the Privacy rule gives us enough information to understand the basic requirements that are required for safeguarding PHI.

Privacy Governs Security

The Privacy rule gives us an understanding that covered entities must safeguard (secure) all identifiable health information held by a covered entity, no matter the form in which it resides. That includes protected health information maintained or communicated on paper, electronically, or orally.

While the Privacy rule globally tells us what is required to protect all health information, the final Security rule will focus on what is required to safeguard protected health information in electronic form.

We will examine a number of areas where the Privacy rule and Privacy Guidelines provide clarification of what requirements covered entities should expect to see in the Security rule to safeguard their protected health information. The Privacy rule addresses and clarifies:

1. Scalability – the Privacy and Security rules are the same no matter what size the entity, however the implementation requirements for small covered entities are much less than what is expected from large covered entities.

2. Access controls - what safeguards a covered entity must implement to control access and disclosure of its protected health information.
3. Audit trails and audit controls - the differences between what is expected from an audit trail or audit control, and what is expected to be provided by an accounting for disclosures of protected health information.

Scalability

Proposed Security Rule

The Security requirements are applicable to all covered entities, from single provider practices to large, national payers, and everything in between. The Security NPRM states that there is no proscribed implementation and that each covered entity must develop its own security implementation, striking a balance between risk and cost of remediation.

Privacy Rule Clarification

In § 164.530(c), the Privacy rule confirms the proposed Security rule's message and adds additional guidance that those protections must be reasonable to protect against unintentional and intentional disclosures that are in violation of the rule. The Privacy rule tells us that each covered entity has the flexibility to develop policies and procedures that are appropriate to that individual entity. In preamble guidance, we not only see reiteration of the proposed Security rule language, but reaffirmation of the scalability expectation that a covered entity must assess its own needs, select implementations appropriate for its own environment and *must* take cost in to consideration.

DHHS provides us with guidance that covered entities can implement safeguards at reasonable cost and the degree of implementation varies with the type and size of the covered entity. (see FR 82562 & 82746). In other words, as stated in the preamble of the Privacy rule, DHHS provides guidance that the intent is that the standards be common sense and scalable. Nor is there any requirement to secure PHI against all threats. Depending on the circumstances, covered entities can rely on policies and procedures to safeguard PHI. If a covered entity has reasonable policies and procedures to prevent theft of PHI, then if PHI is stolen it may not be a violation. DHHS recognizes the reality that it is impossible for any covered entity to be fully secure and provides the flexibility for covered entities to develop their own safeguards.

It is important to note that developing your own safeguards is a process that includes an assessment of risk and documents the decision process used in making risk acceptance and risk avoidance decisions.

Access Controls

Proposed Security Rule

The glossary contained in Addendum 2 of the proposed Security rule essentially defines access controls as methods of controlling and restricting access to prevent unauthorized access to information. The proposed Security rule at § 142.308(i-ii) defines an audit trail as "the data

collected and potentially used in a security audit"). The proposed rule states that covered entities must provide one of three access controls, user based, context based, or role based. In addition, the access controls established must provide a procedure for emergency access. This leaves us with the clear impression that health care providers must have the ability to access needed health information in a crisis. However, we are left on our own to determine the degree or level of implementation and what outcomes are expected.

Privacy Rule Clarification

Fortunately, the final Privacy rule and Privacy Guidelines help us understand what DHHS expects for outcomes and give us plenty of guidance needed to understand access controls. For example, in a response to comment contained in the Privacy rule, (see FR 82716) DHHS states, "Under this regulation, the covered entity's privacy policies will determine who has access to what protected health information. We will make every effort to ensure consistency prior to publishing the final Security Rule."

First, we are told that access control requires role-based access. Under the minimum disclosure provision (see FR 82713 for a discussion on requirements), the Privacy rule clarifies that role based access is required. The Privacy rule further defines that role based access requires policies and procedures that identify the person or class of person within the covered entity that needs access to PHI, to what PHI they require access, and the conditions for which access is granted. It then follows that Security would provide the technological capability to enforce the policies and procedures that define who in the organization can have access to what PHI, for what purposes they can have access, and the conditions for granting access.

Audit Trails

Proposed Security Rule

Audit trails and audit controls are one of the least understood components of the proposed Security rule. While the proposed Security rule states that covered entities must provide audit trails and audit controls, there is little guidance in the proposed rule as to what is expected from an audit trail or audit control.

Audit trails are simply listed as an implementation requirement in the Technical Mechanism portion of the Security rule, under network controls at CFR § A142.308(d)(2)(ii) and defined as "the data collected and potentially used in a security audit".

Audit controls are required under the Technical Services portion of the Security rule, at CFR § 142.308(c)(1)(ii), and defined as "mechanisms employed to examine and record system activity". The preamble (FR page 43254) goes a little further and tells us that audit controls are, "important so that the organization can identify suspect data access activities, assess its security program, and respond to potential weaknesses".

This information has led to speculation that covered entities must identify, track and record every access to protected health information by anyone inside or outside their organization. While

covered entities are free to implement audit controls to that level, and it may make sense with some very large covered entities, the Privacy rule does not support that interpretation.

Privacy Rule Clarification
The Privacy rule provides us with a great deal of help with understanding what is expected from audit trails and audit controls. This insight is found in the response to comments section, Federal Register pages 82739-40.

First DHHS provides differentiation between the requirement to account for disclosures and the requirement for audit trails. On request of the individual, covered entities are required to give individuals an accounting of the disclosure of any PHI that is used to make medical decisions about the individual (a.k.a. designated record set – see §d) that is not for the purpose of treatment, payment, and health care operations (TPO). The information required in this accounting goes beyond what is expected to be contained in an audit trail. The information required is, (1) date of each disclosure, (2) name and address of the person or entity receiving the information, (3) the purpose for which the information is going to be used, and (4) brief description of the information disclosed.

Second, DHHS states that they do not expect audit trails to record every time a user browses or views PHI. What is expected, is that an audit trail record alterations of information; alterations would include edit changes of information, creation of new information, and deletion of information.

Summary

Both the Security NPRM and the final Privacy rule address safeguarding PHI. While the final Security rule will address the security implementations required for protecting information in electronic form, the Privacy rule provides overall guidance in that it requires safeguards for all protected health information, no matter what the media. Since the final Privacy rule also states that the final Security rule will be in alignment with the Privacy rule, we can rely on the guidelines the Privacy rules gives us to also apply to the final Security rule.

The Privacy rule gives sufficient guidance for the health care industry to begin implementing security that will comply with the final Security rule. The required security implementations are scalable and rely on common sense. Each covered entity determines the security implementations that are appropriate for their organization, taking, size, type of business, and cost into consideration. However, each entity should document and justify that those decisions are made on an informed basis, taking into consideration their assessment of threats, impact, and costs of remediation. Security features that present barriers to patient care are not appropriate; delivery of quality patient care retains primacy over privacy and security.

Author Profile Bio

Tom Hanks has over twenty years of information systems, management consulting, and operations experience. He is currently a Director of Client Services in PricewaterhouseCoopers Health Care Practice. Since 1995, Mr. Hanks has been actively contributing expertise to health care industry associations and working with DHHS personnel addressing compliance with HIPAA regulations on privacy, security, and transactions. Mr. Hanks is a board member of WEDi (Workgroup for Electronic Data Interchange), member of the WEDi/SNIP (Strategic National Implementation Plan) steering committee, co-chair of the WEDI Privacy Policy Advisory Group (PAG), the WEDi Security PAG, and the WEDi Communications Interoperability Work Group. He is also a commissioner for EHNAC (Electronic Health Network Accreditation Commission) and chairs its Security Standards Criteria Committee.